

THROUGH 13-957 WC

FILED  
LOGGED  
ENTERED  
RECEIVED  
MAY 10 2013  
CLERK, U.S. DISTRICT COURT  
DISTRICT OF MARYLAND  
DEPUTY

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS**<sup>87</sup>  
**FOR ELECTRONIC STORAGE DEVICES**

**I. Purpose of the Affidavit**

This affidavit is submitted in support of a search warrant for the below listed electronic devices seized pursuant to the execution of federal search warrants at 10820 Hanna Street Suite A Beltsville, MD; 5829 Wyndham Circle Unit 105 Columbia, MD; as well as searches made incident to the arrests of Jennifer SIMS; Leonaldo HARRIS; and Jermaine MCGREGOR on charges of violating 21 U.S.C. §846. The electronic devices are in the possession of HSI located at 40 S. Gay Street, Baltimore, MD and are identified as follows:

- Samsung SCH-U365, MEID Hex A0000039E82183;
- Samsung SGH-T239, IMEI 011841/00/694207/6 (S/N RPCZ501734Y)
- Samsung QX410 laptop, S/N ZYPX93BB203450P
- Samsung SGH T-459 cell phone IMEI353061/03/821265/5, S/N R3XZ459156B
- iPhone 4 Serial Number C8TJTQHHP0V
- Cricket AC3781 flashdrive MEID A0000032C5E938
- T-mobile HTC IMEI 359902042655104
- iPhone 4 with a BLACK PLASTIC AND RUBBER CASE AROUND IT
- Motorola Razr V3 IMEI 356479002058382, MSN E23RGW2K97
- Samsung SGH T-139 IMEI 012944/00/471637/4, S/N R21C55A1LPA
- Motorola EX122, MSN: L33UNY3DTJ, IMEI: 353633D40894470
- Apple iPhone 3 WITH A CRACKED FRONT SCREEN
- Samsung SGH-T139 IMEI: 012404/00/283113/9, S/N RQIZ902944L
- Nokia 2610, IMEI011750/00/722307/3
- Sony Cybershot S/N 0115764
- Samsung SGH-T229, IMEI 357991/02/862416/0, S/N RP6S950324J
- Thumbdrive, S/N 3211KCA
- Sony PCG-7Z1L laptop, Service Tag #C3LQAX4P
- Acer Aspire one D255E-2677, S/N LUSF10D1751030286C1601
- HP G60 laptop S/N 2CE94788G1

Your affiant submits that there is probable cause to believe that these electronic devices contain evidence of violations of 21 U.S.C. §846 – Conspiracy to distribute over 1,000 kilograms of marijuana.

4/26/13

**II. Your Affiant**

I, James Stull, being duly sworn, depose and say:

I am a Special Agent with Homeland Security Investigations (HSI) Baltimore, MD. Furthermore, I have been employed as a federal agent for the past 7 years. I am responsible for conducting criminal investigations regarding violations of law committed against the United States. I am currently employed by the U. S. Department of Homeland Security, Homeland Security Investigations (HSI)<sup>1</sup>, as a Special Agent and have been so since July 2006. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18, U.S.C. § 2510(7) and empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code Section 2516.

As part of my employment with HSI, I attended the Criminal Investigator Training Program, which is a twelve week basic program for all Federal criminal investigators held at the Federal Law Enforcement Training Center in Glynco, Georgia. Additionally, I attended Immigration & Customs Enforcement Special Agent Training, which is an additional eleven weeks of training.

Your affiant is currently assigned to the Baltimore Seaport and Airport – High Intensity Drug Trafficking Area (HIDTA) Group, investigating unlawful acts and violations of federal customs law. In the course of my current employment, I have participated in numerous federal and state narcotics investigations relating to drug trafficking, drug smuggling, and money laundering violations. During the course of those investigations, I have been involved in the use

---

<sup>1</sup> In 2010, Immigration & Customs Enforcement (“ICE”) underwent a re-organization. Several investigative components of the Department of Homeland Security were merged into one investigative agency, called Homeland Security Investigations (“HSI”).

of the following investigative techniques: interviewing informants and cooperating witnesses; conducting physical surveillance; conducting short and long-term undercover operations, including reverse undercover drug operations; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing telephone pen register and caller identification system data; conducting court-authorized electronic surveillance, including wire interceptions; and preparing and executing search warrants that have led to seizures of narcotics, firearms, and other contraband. The information in this affidavit is based on my personal knowledge and information provided to me by other law enforcement officers I have conducted investigations involving alien smuggling, drug smuggling, and immigration document and benefit fraud. Based upon my personal observation, consultation with other Agents, and review of the records, I have learned the following facts:

Based on the foregoing knowledge, training, experience, and participation in investigations involving controlled substances, your Affiant knows that:

Drug traffickers utilize digital cellular telephones to contact their associates, sources of supply (SOS) and their customers. A digital cellular telephone or "Smartphone" (a smart phone is a digital cellular telephone with the added abilities to browse the world wide web, send and receive e-mail and digital media such as pictures and video files, and send MMS or "text" messages) is a portable telephone that may be transported from one place to another and remain operational through the use of a portable battery pack or alternate source. Digital cellular telephones are capable of sending and receiving wire communications, operate as a digital paging and voice mail device, send and receive MMS or "text" messaging, browse the internet, take video movies, still pictures, and voice notes, and allow e-mail to be sent and received.



Digital cellular telephones and or "Smart phones" contain "address books" or a series of stored telephone number which are associated with names either given or nicknames that are assigned by the user of the phone. Digital cellular telephones are not party lines, and each telephone has an assigned telephone number, which may be changed, much the same way as a regular residential telephone. Calls can be made to, or received from a regular telephone, other cellular phones, paging devices, or other facility that can be contacted by a conventional telephone. Digital cellular telephones, as with digital display pagers, permit drug traffickers to remain in constant communication with one another via voice, text messaging and e-mail.

Your affiant knows that information contained in the memory of this phone will provide investigators with: the telephone numbers and digital display codes used by accomplices, aiders and abettors, co-conspirators and participants in these illegal activities; the identities of co-conspirators, customers, and criminal associates based upon subscriber information derived from the retrieved phone numbers and names associated with them; stored text and e-mail messages identifying possible co-conspirator; stored digital images and movies, depicting evidence and fruits of the above listed crime.

Additionally, I know from my knowledge, training, and experience that computer hardware and computer software may be utilized to store records which include but are not limited to those relating to drug trafficking, associate names and addresses, and the identity and location of assets illegally gained through criminal activity.

Based on my knowledge, training, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents or officers to seize most or all of the computer items (hardware, software, and

instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site; and searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code embedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

### **III. Probable Cause**

On April 17, 2013, the Pennsylvania State Police received information regarding two suspicious freight pallets that had arrived at YRC Freight located at 100 Roadway Drive, Carlisle, PA 17013 from OC Box Zone located at 211 West Katella Avenue Suite D, Orange, CA

92867. YRC Security stated that during a routine internal inspection of freight to confirm that the freight received matches the bill of lading. A YRC inspector had identified a green leafy substance they believed to be marijuana present in the parcels. YRC Security contacted Pennsylvania State Police who responded to the facility and conducted a field test of the green leafy substance. A NIK field test kit was utilized in the test and the result indicated a positive presumptive result of marijuana. Trooper Mearkle of the Pennsylvania State Police and his certified K-9 "Zigi" conducted a scan of the pallets. "Zigi" was first run on a lineup of five unrelated parcels, and did not give a positive alert while conducting this scan. Then one of the target pallets was placed into the lineup and "Zigi" then ran the line-up again. At this time, "Zigi" gave a positive alert for the presence of a controlled dangerous substance inside of the pallet. Pennsylvania State Police then contacted members of the Maryland State Police Western Maryland Package Interdiction Unit regarding the aforementioned shipment of marijuana that had been encountered at the YRC Freight Company facility located at 100 Roadway Drive, Carlisle, PA 17013. The intended destination of the shipment is manifested as Auto Tech 10820 Hannah Street Suite A, Beltsville, MD 20705. Record checks conducted on the address as well as personal observation of HSI Special Agents reveal that the proper spelling of the street name is Hanna Street. The Maryland State Police Western Maryland Package Interdiction Unit then traveled to the aforementioned YRC freight facility to take custody of the two pallets in order to conduct a controlled delivery to the intended address. The Maryland State Police Western Maryland Package Interdiction Unit applied for a Search and Seizure Warrant in the State of Maryland for the two pallets obtained from YRC Freight. A partial search was conducted in order to maintain the overall integrity of the packaging in order to facilitate a controlled delivery.

The partial search identified approximately 216 pounds of a green leafy substance believed to be marijuana. A test of the aforementioned substance was performed and was shown to be a presumptive positive for the presence of marijuana. Based on the remaining boxes as well as the packing method utilized by the shipper Maryland State Police Officers as well as HSI Special Agents believe the total amount of marijuana present to be in excess of 1000 pounds. This is supported by the fact that the approximate weight of the pallets was 1024 pounds and 924 pounds respectively.

HSI Special Agents conducted surveillance on the delivery address of 10820 Hanna Street Suite A, Beltsville, MD 20705. HSI Agents observed a sign above the property clearly labeled Auto Tech & HP Group Services as well as large white number on the door identifying the address as the same. Additional record checks conducted on the address through various law enforcement databases were negative.

On April 18, 2013, Special Agent Stull obtained a search and seizure warrant in the District of Maryland for the aforementioned address of 10820 Hanna Street Suite A; Beltsville, MD. On April 18, 2013, your affiant as well as additional Agents of HSI Baltimore; members of the Maryland State Police Western Maryland Package Interdiction Unit; and members of the Prince Georges County Police Department Narcotics Enforcement Division conducted a controlled delivery of marijuana to 10820 Hanna Street Suite A, Beltsville, MD 20705. Prior to the execution of the controlled delivery while conducting surveillance HSI Special Agents identified two vehicles. A red Hyundai with Maryland license plate 3BA6028 as well as a white cargo van bearing Texas license plate ASO-1055 were spotted in the vicinity of the address. Surveillance observed that the driver of the Hyundai was a female wearing green pants and a



white shirt. The female exited the vehicle approached two black males who were sitting in the white cargo truck. One black male then exited the van and entered into the red Hyundai. The two vehicles departed the location. The aforementioned female then produce a set of keys and made entry into the target address.

At approximately 1335 hours the controlled delivery commenced. The freight was accepted and signed for by an individual later identified as Jennifer N. SIMS date of birth October 15, 1982; SIMS was the female previously observed entering the structure wearing green pants and a white shirt. During that time both of the aforementioned vehicles were observed in the area of 10820 Hanna Street Suite A, Beltsville, MD 20705. After successful delivery of the pallets, the call was made to stop the drivers of the two vehicles. The driver of the white van Jermaine J. McGregor date of birth August 10, 1978 was stopped without incident. The driver of the red Hyundai failed to yield for Officers and led officers on a short high speed pursuit until they were ultimately apprehended. The driver of that vehicle was later identified as Leonaldo A. Harris with a date of birth of May 2, 1981.

Jermaine McGregor was read his rights and waived those rights and chose to speak to law enforcement. McGregor stated that he and Harris had been friends for a long period of time. McGregor stated that Harris had offered him work if he came up to Maryland from Florida which is where McGregor was living at the time. McGregor stated that he was at 10820 Hanna Street Suite A, Beltsville, MD to assist Harris in transporting marijuana to a location unknown to him. McGregor stated that prior TO April 18<sup>th</sup>, 2013, himself and Harris had been in Los Angeles, CA purchasing marijuana for shipment back to Maryland. McGregor stated that he and Harris had traveled to Los Angeles, CA with approximately \$200,000 usd in cash with the



purpose of purchasing narcotics for shipment to Maryland. McGregor stated that Harris utilized several individuals to transport currency in bulk to Los Angeles, CA for the purpose of purchasing marijuana for shipment to Maryland.

McGregor stated that on this particular trip they had purchased approximately 1100 to 1300 pounds of marijuana. McGregor further stated that the two then traveled to a home in the Los Angeles, CA metropolitan area owned and or rented by Harris with the narcotics for the purpose of packing the contraband for shipping to Maryland. McGregor stated that he assists Harris off and on and that he has conducted this type of transaction once monthly since the beginning of 2013.

After all three individuals and the location were secured; a search warrant of the location was executed. A search of the premises resulted in the seizure of a scale which is utilized by drug traffickers to weigh out their products for further distribution and sale. Additionally it appeared that the facility was utilized for the express purpose of receiving; breaking down; and redistributing contraband as there was no evidence of business taking place at the location. Additionally there were indications that previous shipments have been received at that location. Further a total of 1356 pounds of marijuana was seized from the pallets that were accepted for delivery by Jennifer SIMS packaged and shipped by Leonaldo HARRIS and Jermaine MCGREGOR to 10820 Hanna Street Suite A, Beltsville, MD 20705.

While Jennifer SIMS was speaking with Agents she provided a current address for Leonaldo HARRIS of 5829 Wyndham Circle Columbia, MD. Prior to her being transported to the Baltimore City Detention Center Sims was transported to the aforementioned address in

order to obtain prescription medication that she takes on a daily basis. Additionally Sims has a child and she was obtaining clothing for the care of her child.

Officers escorted Sims to 5829 Wyndham Circle Columbia, MD in order to obtain the medication and clothing. Sims granted consent for Officers to enter the premises. Officers approached and Sims parked in front of an unmarked white garage style door in the complex. Sims was in possession of a garage door opener that caused the aforementioned garage door to open. Upon entry into the garage Officers observed two large boxes which were consistent with containers found at 10820 Hanna Street Suite A Beltsville, MD during a federal search warrant executed early that day. Federal authorities seized 1356 pounds of marijuana from the aforementioned located. As Officers passed the boxes they smelled based on training and experience what they recognize to be consistent with the odor of un-burnt marijuana emanating from the aforementioned boxes located in the garage of the unit.

As Sims was escorted through the location to obtain her medicine and clothing for her child Officers observed suitcases with men's clothing bearing the first five letters of "Leona" and a tag from United Airlines Flight 1279 departing from Los Angeles International Airport and arriving at Baltimore Washington International airport on April 17, 2013. Sims as well as McGregor stated that Harris flew back into Baltimore from Los Angeles on April 17, 2013.

During the execution of the search warrant at 5829 Wyndham Circle Unit 105 Columbia, MD officers identified various items of interest to include an additional quantity of a green leafy substance that tested positive for the properties of marijuana; a loaded Glock 19 firearm; ammunition; firearm magazines; an abundance of banking information from various financial institutions; various cellular telephones and computers; as well as a money counter.

**TIME AND TECHNICAL REQUIREMENTS FOR COMPUTER SEARCHES**

Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them.

Based upon my knowledge, and information received from other law enforcement officers, I know that searching for information from computers requires a qualified computer expert in a laboratory or other controlled environment for a considerable amount of time. This is true because of the following:

- a. **The volume of evidence.** Computer storage devices (like hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of millions of pages of information. For example, one megabyte of magnetic media can store approximately 312 pages of text, resulting in a stack of paper 1.6 inches thick. A 40 gigabyte hard drive, common in many new personal computer systems today, could store approximately 12.48 million pages of text, resulting in a stack of paper approximately 5,333 feet high. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence of instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.
- b. **Technical requirements.** Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files, including that which has been deleted specifically to defeat law enforcement evidence collection efforts,. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (from either external sources or from destructive codes imbedded in the system as a "booby



trap"), a controlled environment is essential to its complete and accurate analysis.

#### IV. Conclusion

Based on my training and experience, in investigating drug trafficking/smuggling organizations, I know that drug traffickers/smugglers involved in the smuggling of large quantities of controlled substances frequently resort to using computers; cellular/digital phones; smart phones as well as other electronic storage devices to keep in contact with members of the organization in order to communicate their locations and advise of their status while transporting drugs in order to shield the shipment of drugs from detection by law enforcement and loss from theft. Drug traffickers/smugglers further utilize computers as well as other electronic storage devices to keep/maintain records of their illegal business activities. For these reasons, the stored text, text files, SMS, MMS, and e-mail messages, alpha-numeric messages and stored telephone numbers, names, and addresses and other stored electronic data not limited to pictures, GPS data and website information, text data, notes, etc. are evidence of violations of 21 U.S.C. §846 – Conspiracy to distribute and possess with intent to distribute 1000 kilograms or more of marijuana.

Therefore, based on the aforementioned facts, I believe that there is probable cause that the seized electronic devices have been used in furtherance of illegal drug trafficking activities in violation of 21 U.S.C. §846. Further, there is probable cause to believe that information stored on the aforementioned electronic devices identify other individuals involved in violations of federal narcotics laws. Therefore, I am seeking authorization to search, access, and retrieve all electronically stored data contained in the below listed items:

On April 18, 2013, the following electronic media were seized from Jermaine McGregor

subsequent to his arrest:

- Samsung SCH-U365, MEID Hex A0000039E82183;
- Samsung SGH-T239, IMEI 011841/00/694207/6 (S/N RPCZ501734Y)

On April 18, 2013, the following electronic media were seized from Jennifer Sims subsequent to her arrest at 10820 Hanna St., Suite A, Beltsville, MD:

- Samsung QX410 laptop, S/N ZYPX93BB203450P
- Samsung SGH T-459 cell phone IMEI353061/03/821265/5, S/N R3XZ459156B
- iPhone 4 Serial Number C8TJTQHHP0V
- Cricket AC3781 flashdrive MEID A0000032C5E938

On April 18, 2013, the following electronic media were seized from Leonaldo Harris subsequent to his arrest:

- T-mobile HTC IMEI 359902042655104
- iPhone 4 with a BLACK PLASTIC AND RUBBER CASE AROUND IT
- Motorola Razr V3 IMEI 356479002058382, MSN E23RGW2K97
- Samsung SGH T-139 IMEI 012944/00/471637/4, S/N R21C55A1LPA

On April 19, 2013, the following electronic media were seized during the execution of a federal search warrant at the residence of Leonaldo Harris and Jennifer Sims, 5829 Wyndham Circle, Columbia, Maryland:

- Motorola EX122, MSN: L33UNY3DTJ, IMEI: 353633D40894470
- Apple iPhone 3 WITH A CRACKED FRONT SCREEN
- Samsung SGH-T139 IMEI: 012404/00/283113/9, S/N RQIZ902944L
- Nokia 2610, IMEI011750/00/722307/3
- Sony Cybershot S/N 0115764
- Samsung SGH-T229, IMEI 357991/02/862416/0, S/N RP6S950324J
- Thumbdrive, S/N 3211KCA
- Sony PCG-7Z1L laptop, Service Tag# C3LQAX4P
- Acer Aspire one D255E-2677, S/N LUSF10D1751030286C1601
- HP G60 laptop S/N 2CE94788G1

I, Special Agent James Stull, affirm under penalties of perjury that the facts and circumstances recounted in the foregoing affidavit are true and accurate to the best of my knowledge.



James Stull, Special Agent  
Homeland Security Investigations

Subscribed and sworn before me on April 26 2013.



William Connelly  
Chief United States Magistrate Judge

4  
95  
4/26/13



**ATTACHMENT A**  
**DESCRIPTION OF PREMISES TO BE SEARCHED**

On April 18, 2013, the following electronic media were seized from Jermaine McGregor subsequent to his arrest:

- Samsung SCH-U365, MEID Hex A0000039E82183;
- Samsung SGH-T239, IMEI 011841/00/694207/6 (S/N RPCZ501734Y)

On April 18, 2013, the following electronic media were seized from Jennifer Sims subsequent to her arrest at 10820 Hanna St., Suite A, Beltsville, MD:

- Samsung QX410 laptop, S/N ZYPX93BB203450P
- Samsung SGH T-459 cell phone IMEI353061/03/821265/5, S/N R3XZ459156B
- iPhone 4 Serial Number C8TJTQHHP0V
- Cricket AC3781 flashdrive MEID A0000032C5E938

On April 18, 2013, the following electronic media were seized from Leonaldo Harris subsequent to his arrest:

- T-mobile HTC IMEI 359902042655104
- iPhone 4 with a BLACK PLASTIC AND RUBBER CASE AROUND IT
- Motorola Razr V3 IMEI 356479002058382, MSN E23RGW2K97
- Samsung SGH T-139 IMEI 012944/00/471637/4, S/N R21C55A1LPA

On April 19, 2013, the following electronic media were seized during the execution of a federal search warrant at the residence of Leonaldo Harris and Jennifer Sims, 5829 Wyndham Circle, Unit 105, Columbia, Maryland:

- Motorola EX122, MSN: L33UNY3DTJ, IMEI: 353633D40894470
- Apple iPhone 3 WITH A CRACKED FRONT SCREEN
- Samsung SGH-T139 IMEI: 012404/00/283113/9, S/N RQIZ902944L
- Nokia 2610, IMEI011750/00/722307/3
- Sony Cybershot S/N 0115764
- Samsung SGH-T229, IMEI 357991/02/862416/0, S/N RP6S950324J
- Thumbdrive, S/N 3211KCA
- Sony PCG-7Z1L laptop, Service Tag# C3LQAX4P
- Acer Aspire one D255E-2677, S/N LUSF10D1751030286C1601
- HP G60 laptop S/N 2CE94788G1

**ATTACHMENT B**  
**DESCRIPTION OF ITEMS TO BE SEIZED**

1. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, video recording devices, video recording players, electronic information storage devices, monitors, and or televisions, flatbed scanners, and data where instrumentalities of and will contain evidence related to this crime. The following definitions apply to the terms as set out in this affidavit and attachment:

(1) Computer hardware

Computer hardware consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, optical, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to central processing units; internal and peripheral storage devices such as fixed hard disks, external hard drives, floppy disk drives and diskettes, USB thumb drives, copiers, memory cards, CDs, DVDs and other data and memory storage devices); iPads and other tablet computers, peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

(2) Computer Software

Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It includes programs to run operating systems, applications, and utilities.

(3) Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

(4) Passwords and Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security

*JS*  
*4/26/13*

devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touches. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

#### (5) Recordable Media

Any and all CD, DVD, Blu-Ray or other recordable media disks, USB thumb drives, floppy disks, MP3 players, iPods or other music and video recording devices, digital audio recorders, digital cameras and the media it records to including CDs, DVDs, media cards and video tape, cell phones and the memory cards used by cell phones, GPS navigation units, tape backup units and their media, Xbox, Playstation and all gaming consoles. Recordable media includes any device capable of receiving data from any electronic source for storage, analysis, transmission or display.

The computers may be searched for the following items:

- a. lists of customers and related identifying information;
  - b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
  - c. any information related to sources of narcotic drugs (including photographs, names, addresses, phone numbers, or any other identifying information);
  - d. any information recording travel schedules or travel;
  - e. all bank records, checks, credit card bills, account information, and other financial records;
  - f. all of the names, telephone numbers, stored numeric, and/or text messages contained, images, website information.
2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as



logs, phonebooks, saved usernames and passwords, documents, and browsing history

WGC  
4/26/13